IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Case No. 3:19cr19**
	)	
TROY GEORGE SKINNER,	)	
Defendant	)	

MOTION TO SUPPRESS EVIDENCE

Troy Skinner, through counsel, moves the Court to suppress images and videos the government obtained from his Google accounts and his cell phone in violation of the Fourth Amendment.

BACKGROUND

In approximately December 2017, Mr. Skinner "met" a young American woman online through a gaming platform called Discord. The platform allows users of the platform to "chat" with each other. The users can message each other in the platform to have a typed "conversation." The users can also talk with each other while on a video call. [redacted] Mr. Skinner truthfully told the young woman that he was twenty-four years old. In New Zealand, where Mr. Skinner was born, raised, and spent his entire life until coming to the United States in June 2018, the age one can legally consent to sexual activities is

[redacted]

sixteen years. In New Zealand, reasonable mistake of age is a defense to sexual conduct with a person under sixteen years old.

[redacted] The government seized the image described in Count Eight and the video described in Count Nine of the indictment from Mr. Skinner's digital Google accounts and not from any device. The government seized the video described in Count Seven of the indictment from Mr. Skinner's cell phone (and later from his desktop computer in New Zealand), which the government took upon Mr. Skinner's arrest in Virginia. Mr. Skinner never shared these images or videos with anyone else. There is no indication at all that Mr. Skinner ever produced or possessed any other alleged child pornography.

ARGUMENT

I. The Court should suppress evidence seized pursuant to the search warrants in 3:18-SW-180, 3:18-SW-267, and 3:18-SW-268.

The warrants in this case for Mr. Skinner's phone and his Google accounts were essentially general warrants. They did not establish probable cause sufficient to authorize a wholesale search for all information on the phone or in the accounts. [redacted] But they provided no basis to suspect that Mr. Skinner had

communicated with any other minor individual. Instead of particularly describing the specific evidence for which probable cause existed, the warrant's scope was breathtakingly broad.

The warrant for the cell phones, 3:18-SW-180 attached as Exhibit C, authorized the seizure of such broad categories as: "All records and information relating to the location, past or present, of" Mr. Skinner; "All records relating to" Mr. Skinner's "Internet search and online shopping histories;" "Any and all visual depictions of minors;" "Any and all address books, names, and lists of names and addresses of minors;" and "Any and all information relating to any and all Discord accounts/usernames used by TROY GEORGE SKINNER[.]" It further authorized the seizure of "records of, or information about the [phones'] Internet activity, including firewall logs, caches, browser history and cookies, . . . search terms that the user entered into any Internet search engine, and records of user-typed web addresses."

The warrants for the Google accounts information, 3:18-SW-267 and 3:18-SW-268 attached as Exhibits A and B, are broader still. They authorized seizure of the "contents of all emails" regardless of from or to whom they were sent or when. They authorized seizure of "[a]ny and all contents stored in the Google Drive account" regardless of its nature. They authorized seizure of "All records or other information stored at any time by an individual using the account including address books, contact and buddy lists, calendar data, pictures, and files." Basically, like a warrant for "all objects" in a house, these warrants authorized a wholesale seizure of the entire contents of the account, to be sifted by law enforcement. The warrants for the Google accounts, further, were based on the information found pursuant to an execution of the warrant for Mr. Skinner's cell phones.

A. Privacy Interests at Stake

The Supreme Court has held that through a cell phone, the "sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions." *Riley v. California*, 134 S. Ct. 2473, 2489 (2015). "[T]here is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception." *Id.* at 2490. "A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Id.* at 2491.

B. Particularity

The Fourth Amendment provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but **upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized**.

U.S. CONST. Amend. IV (emphasis added). The objective of the particularity and probable cause requirements of the Fourth Amendment "is that those searches deemed necessary should be as limited as possible." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

Particularity and overbreadth are related concepts—both essentially depend on the scope of probable cause and whether the entire set of described items for which seizure is authorized fit within the scope of probable cause. "Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993). "The two separate rules must both be met since an unnecessary invasion of privacy

can occur either when the magistrate has a firm command of the doctrine of probable cause and a poor command of the English language, or vice versa." *United States v. Weber*, 923 F.2d 1338, 1342 (9th Cir. 1990).

"[G]eneric classifications in a warrant are acceptable only when a more precise description is not possible." *United States v. Bright*, 630 F.2d 804, 812 (5th Cir. 1980); *see also United States v. Dickerson*, 166 F.3d 667 (4th Cir. 1999) ("the law of this Circuit does allow some discretion to the officers executing a search warrant, so long as the warrant at least minimally confines the executing officers' discretion by allowing them to seize only evidence of a particular crime"), reversed on other grounds; *Montilla Records of Puerto Rico v. Morales*, 575 F.2d 324, 326 (1st Cir.1978) (observing that the greater the feasibility of a precise, specific description in a warrant, the less justifiable the employment of a general or generic description). Here, the government did not even attempt to narrow the scope of the objects and information it sought to fit the scope of probable cause established by the affidavits. It did not restrict its search to, for example, communications between V1 and Mr. Skinner. It did not at all reflect the documents which the government's interview of V1 provided them reason to believe existed.

One way that the government frequently uses to escape this limiting principle is by offering profile evidence. That is, it offers evidence that the suspect fits a profile that shares common criminal characteristics, and thereby establishes probable cause for a larger sphere of evidence common to that class of criminals. *See, e.g., United States v. Aguilar*, 825 F.2d 39, 41 (4th Cir. 1987) (finding that defendant matched drug courier profile). First, the Google warrant applications did not even proffer any type of profile. *See* Exs. A and B. For the cell phone warrant, the government copied and pasted into the warrant application its frequently-reused boilerplate describing the common characteristics of child pornography collectors. *See* Ex. C, Affidavit at 6.

However, the affidavit fails at a key point. The facts asserted must place the suspect within the definition of the profile that is proffered. Nothing in the affidavit places Mr. Skinner within the collector profile described in the warrant. Child pornography collectors, the affidavit avers, receive sexual stimulation and satisfaction from contact with children. [redacted] It also states that collectors keep their materials in a variety of media, also collect erotica, use the materials to seduce children, correspond and share with other collectors, and prefer not to be without their child pornography for any prolonged period. None of these factors fits the information the agent provided to the magistrate in the affidavit about Mr. Skinner.

Thus, the Court here is in the same position as the Ninth Circuit in *United States v. Weber*, 923 F.3d 1338 (9th Cir. 1990). Two years before the warrant, agents intercepted a package containing child pornography addressed to the defendant. *Id.* at 1340. The defendant responded to a government-created ad for child pornography and ordered it delivered to his house. It was delivered and agents obtained a search warrant for the house to seize not only the delivered pictures but video equipment, address books, diaries, and correspondence for any other (unknown) orders. *Id.* at 1341. The agent recited what he believed were the typical practices of child pornography collectors. The defendant did not dispute that probable cause existed for the pictures he had ordered in response to the ad, *see id.* at 1343, but disputed the breadth of the warrant for other evidence, and the Ninth Circuit agreed. "[P]robable cause to believe that some incriminating evidence will be present at a particular place does not necessarily mean there is probable cause to believe that there will be more of the same." *Id.* at 1344; *see also United States v. Church*, 232 F. Supp. 3d 831, 841 (E.D. Va. 2017) ("The argument appears to be that, when a suspect sends a text

message during the commission of an alleged offense, police automatically have probable cause to seize any and all electronics that the suspect owns, to search those electronics indiscriminately, and to do so without first presenting evidence that the additional electronics are relevant to the crime allegedly committed. All of this is permissible, the United States argues, because of the 'integrated nature of the modern computer network.' This post-hoc argument was unpersuasive when it was first asserted to defend the warrant, and it remains unpersuasive as an attempt to justify the seizure under the guise of consent."). This limiting principle is why the government provides profile evidence in many of its warrant applications—to show probable cause that additional evidence may be present and subject to seizure, based on the defendant's fitting the profile of a child pornography collector, for example, or a drug courier.

C. Scope of Probable Cause

A court reviewing the validity of a search warrant after a search must "conscientiously review the sufficiency of affidavits on which warrants are issued." *Gates*, 462 U.S. at 239. The affidavit must, of course, establish probable cause that a crime has been committed. U.S. Const. Amend. IV. But more than that, it cannot rely on even a class of crimes, but be tied to a particular crime. It must relate to "a specific illegal activity." *United States v. Dickerson*, 166 F.3d 667, 694 (4th Cir. 1999) rev'd on other grounds by *Dickerson v. United States*, 530 U.S. 428 (2000). The warrant that issues as a result of the affidavit, in turn, must "confine[] the executing officers' discretion by allowing them to seize only evidence of a particular crime." *United States v. Fawole*, 785 F.2d 1141, 1144 (4th Cir. 1986). And a particular crime does not simply mean a particular statute, but includes the way in which the officers suspect it was violated in the instant case. *See Dickerson*, 166 F.3d at 694 ("a specific illegal activity").

Many Circuit Courts of Appeal have held that warrants authorizing searches for violations of even named criminal statutes do little or nothing to limit the searching officers' discretion. *See United States v. Abrams*, 615 F.2d 541, 542–43 (1st Cir.1980) (finding warrant limited only by reference to records and federal fraud statute is overbroad); *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992) ("Mere reference to 'evidence' of a violation of a broad criminal statute or general criminal activity provides no readily ascertainable guidelines for the executing officers as to what items to seize."); *Rickert v. Sweeney*, 813 F.2d 907, 909 (8th Cir.1987) (finding warrant limited only by references to the general conspiracy statute and general tax evasion statute did "not limit the search in any substantive manner"); *United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982) ("'[L]imiting' the search to only records that are evidence of the violation of a certain statute is generally not enough."); *United States v. Leary*, 846 F.2d 592 (10th Cir. 1988) (same).

So, for example, in *United States v. Gardner*, 537 F.2d 861 (6th Cir. 1976), the warrant authorized a search for "all firearms and ammunition." *Id.* at 862. But the Sixth Circuit concluded that the affidavit only established probable cause "solely for a .38 caliber pistol that was allegedly used in an armed robbery and murder." *Id.* Therefore, the warrant authorizing a search for all firearms was fatally overbroad. *Id.* Here, the warrants did not incorporate the affidavits; and they did nothing to narrow the breadth of the information for which seizure was authorized or tie them to the scope of the probable cause that they had. Attachment B of both warrants simply recited the names of the statutes for which the government believed probable cause existed and did not describe the particular violations or evidence it expected to find based on the facts developed.

D. Severability

If the Court finds the need to examine whether the warrants are severable, it should conclude that they are not. "Severability can apply to a warrant with invalid portions 'only if the

valid portions of the warrant [are] sufficiently particularized, distinguishable from the invalid portions, and make up the greater part of the warrant.'" *United States v. Sells*, 463 F.3d 1148, 1151 (10th Cir. 2006) (quoting *United States v. Naugle*, 997 F.3d 819, 822 (10th Cir. 1993)); *United States v. Sykes*, No. 2016 WL 8291220, at *17 (E.D.N.C. Aug. 22, 2016), report and recommendation adopted, 2016 WL 6882839 (E.D.N.C. Nov. 22, 2016). Here, the warrants only list broad categories of materials, all of which are broader than the scope of probable cause, and none of which particularly describe the set of information for which probable cause existed. It is therefore impossible to "divide the warrant into individual phrases, clauses, paragraphs, or categories of items" and identify one or more that are sufficiently particularized and supported by probable cause. *Sells*, 463 F.3d at 1155. The warrant is not subject to severability and the entire fruits of the searches pursuant to the warrants should be suppressed under the Fourth Amendment.

II. The extended seizure of Mr. Skinner's cell phone before obtaining the search warrant was unreasonable.

In this case, the officers seized Mr. Skinner's phone on June 22, 2018. They obtained the warrant to search his phone on July 20, 2018—twenty-nine days later. Such an extended seizure was unreasonable under the Fourth Amendment. *See United States v. Pratt*, 915 F.3d 266 (4th Cir. Feb. 8, 2019). In *Pratt*, the government investigated Mr. Pratt for allegedly running a prostitution ring that included minor children. During a conversation with Mr. Pratt, the officers seized his cell phone. The officers did not get a search warrant for the phone until thirty-one days after seizing it. Relying on an Eleventh Circuit case that found a twenty-one day delay between the seizure and subsequent search of a computer unreasonable, the Fourth Circuit held that the thirty-one day delay in *Pratt* was unreasonable because the officers had "failed to exercise diligence by spending a whole month debating where to get a warrant." *Id.* at 272. Similarly, here, the government's twenty-nine day delay in obtaining a warrant for Mr. Skinner's cell phone

after initially seizing it is unreasonable under the Fourth Amendment. The Court should suppress the contents of Mr. Skinner's cell phone that the government illegally seized.

CONCLUSION

Thus, the Court should suppress images and videos the government obtained from Mr. Skinner's Google accounts and his cell phone in violation of the Fourth Amendment.

Respectfully submitted,
TROY GEORGE SKINNER

By: _____/s/_____

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

Robert Wagner
Va. Bar No. 27493
Office of the Federal Public Defender
701 East Broad Street, Suite 3600
Richmond, VA 23219
Ph. (804) 565-0808
Fax (804) 648-5033
robert_wagner@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on January 10, 2020, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

_____/s/_____

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org